

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the subject application.

Listing of Claims:

1. (original) A transaction system for performing secure transactions over a communication network comprising:

a merchant server system including a computer processor and associated memory, said merchant server system offering items for sale;

a buyer system including a computer processor and associated memory, said buyer system being selectively couplable to said merchant server system over said communication network to initiate a transaction, wherein, during said transaction, said buyer system selects one or more of said items for purchase;

a security server system including a computer processor and associated memory and an encryption device, said security server system receiving buyer information from said buyer system, encrypting said buyer information in an encryption key that prevents said merchant server system from decrypting said buyer information, and transferring said encrypted buyer information to said merchant server system; and

a third server system including a computer processor and associated memory, said third server system being selectively couplable to said merchant server system, wherein said merchant server system transmits at least a portion of said encrypted buyer information to said third server system for processing during said transaction.

2. (original) The transaction system of claim 1 wherein said third server system is one of a delivery server system and a payment processor server system.

3. (original) The transaction system of claim 2 wherein said encrypted buyer information received by said delivery server system is delivery address information of said buyer.
4. (original) The transaction system of claim 2 wherein said encrypted buyer information received by said payment processor server system is payment information of said buyer.
5. (original) The transaction system of claim 1 further comprising a fourth server system including a computer processor and associated memory, said fourth server system being selectively couplable to one of said merchant server system and said third server system, wherein said one of said merchant server system and said third server system transmits at least a portion of said encrypted buyer information to said fourth server system for processing during said transaction.
6. (original) The transaction system of claim 5 wherein said security server system encrypts said buyer information into a first document and a second document, wherein said first document is transmitted to said third server system by said merchant server system and said second document is transmitted to said fourth server system by said merchant server system.
7. (original) The transaction server system of claim 5 wherein said security server system encrypts said buyer information into a first document and a second document, wherein said first and second documents are transmitted to said third server system by said merchant server system and said second document is transmitted to said fourth server system by said third server system.
8. (original) The transaction system of claim 6 wherein said third server system is one of a delivery server system and a payment processor server system and wherein said fourth server system is the other of said delivery server system and said payment processor server system, and wherein said first document contains one of the buyer system's delivery address information and

the buyer system's payment information and the second document contains the other of said buyer system's delivery address information and said buyer system's payment information.

9. (original) The transaction system of claim 8 wherein said security server system encrypts said first document using a first encryption key and said second document using a second encryption key, wherein said one of said third server system and said fourth server system that receives said first document can decrypt said first document but not said second document and wherein said other one of said third server system and said fourth server system that receives said second document can decrypt said second document but not said first document.

10. (original) The transaction system of claim 7 wherein said third server system is one of a delivery server system and a payment processor server system and wherein said fourth server system is the other of said delivery server system and said payment processor server system, and wherein said first document contains one of the buyer system's delivery address information and the buyer system's payment information and the second document contains the other of said buyer system's delivery address information and said buyer system's payment information.

11. (original) The transaction system of claim 10 wherein said security server system encrypts said first document using a first encryption key and said second document using a second encryption key, wherein said one of said third server system and said fourth server system that receives said first document and second documents from said merchant server system can decrypt said first document but not said second document and wherein said other one of said third server system and said fourth server system that receives said second document can decrypt said second document but not said first document.

12. (amended) A system for performing secure transactions over a communication network comprising:

a merchant server system including a computer processor and associated memory, said merchant server system offering items for sale;

a buyer system including a computer processor and associated memory, said buyer system being selectively couplable to said merchant server system over said communication network to initiate a transaction, wherein, during said transaction, said buyer system selects one or more of said items for purchase;

a security server system including a computer processor and associated memory, said security server system being selectively couplable to said buyer system to receive buyer information from said buyer system in the course of said transaction, said buyer information including delivery address information and payment information;

a delivery server system including a computer processor and associated memory; and
a payment processor server system including a computer processor and associated memory;

wherein said security server encrypts and transmits said delivery address information to said delivery server system and said payment information to said payment processor server system.

13. (original) The transaction system of claim 12 wherein said security server system encrypts said delivery address information into a first document and encrypts said payment information into a second document.

14. (original) The transaction system of claim 13 wherein said security server system transmits said first and second documents to said merchant server system, which transmits said first document to said delivery server system and said second document to said payment processor server system; and

wherein said merchant server system is incapable of decrypting said first and second documents.

15. (original) A transaction system for performing secure transactions over a communication network comprising:

a merchant server system including a computer processor and associated memory, said merchant server system offering items for sale;

a buyer system including a computer processor and associated memory, said buyer system being selectively couplable to said merchant server system over said communication network to initiate a transaction, wherein, during said transaction, said buyer system selects one or more of said items for purchase and transmits information regarding said one or more items to said merchant server system;

a security server system including a computer processor and associated memory and an encryption device, said security server system receiving buyer information from said buyer system, encrypting said buyer information in an encryption key that prevents said merchant server system from decrypting said buyer information, and transferring said encrypted buyer information to said merchant server system; and

a third server system including a computer processor and associated memory, said third server system being selectively couplable to said merchant server system, wherein said merchant server system transmits at least a portion of said encrypted buyer information to said third server system for processing during said transaction.

16. (original) The transaction system of claim 15 wherein said third server system is one of a delivery server system and a payment processor server system.

17. (original) The transaction system of claim 16 wherein said encrypted buyer information received by said delivery server system is delivery address information of said buyer.

18. (original) The transaction system of claim 16 wherein said encrypted buyer information

received by said payment processor server system is payment information of said buyer.

19. (original) The transaction system of claim 15 further comprising a fourth server system including a computer processor and associated memory, said fourth server system being selectively couplable to one of said merchant server system and said third server system, wherein said one of said merchant server system and said third server system transmits at least a portion of said encrypted buyer information to said fourth server system for processing during said transaction.

20. (original) The transaction system of claim 19 wherein said security server system encrypts said buyer information into a first document and a second document, wherein said first document is transmitted to said third server system by said merchant server system and said second document is transmitted to said fourth server system by said merchant server system.

21. (original) The transaction server system of claim 19 wherein said security server system encrypts said buyer information into a first document and a second document, wherein said first and second documents are transmitted to said third server system by said merchant server system and said second document is transmitted to said fourth server system by said third server system.

22. (original) The transaction system of claim 20 wherein said third server system is one of a delivery server system and a payment processor server system and wherein said fourth server system is the other of said delivery server system and said payment processor server system, and wherein said first document contains one of the buyer system's delivery address information and the buyer system's payment information and the second document contains the other of said buyer system's delivery address information and said buyer system's payment information.

23. (original) The transaction system of claim 22 wherein said security server system encrypts

said first document using a first encryption key and said second document using a second encryption key, wherein said one of said third server system and said fourth server system that receives said first document can decrypt said first document but not said second document and wherein said other one of said third server system and said fourth server system that receives said second document can decrypt said second document but not said first document.

24. (original) The transaction system of claim 21 wherein said third server system is one of a delivery server system and a payment processor server system and wherein said fourth server system is the other of said delivery server system and said payment processor server system, and wherein said first document contains one of the buyer system's delivery address information and the buyer system's payment information and the second document contains the other of said buyer system's delivery address information and said buyer system's payment information.

25. (original) The transaction system of claim 24 wherein said security server system encrypts said first document using a first encryption key and said second document using a second encryption key, wherein said one of said third server system and said fourth server system that receives said first document and second documents from said merchant server system can decrypt said first document but not said second document and wherein said other one of said third server system and said fourth server system that receives said second document can decrypt said second document but not said first document.

26. (original) A system for performing secure transactions over a communication network comprising:

a merchant server system including a computer processor and associated memory, said merchant server system offering items for sale;

a buyer system including a computer processor and associated memory, said buyer system being selectively couplable to said merchant server system over said communication network to initiate a transaction, wherein, during said transaction, said buyer system selects one or more of said items for purchase;

a security server system including a computer processor and associated memory and an encryption device, said security server system receiving buyer information from said buyer system and forming a merchant document including information regarding the item being purchased, encrypting said buyer information into a payment document including the buyer's payment information and encrypting said buyer information into an address document including the buyer's shipping address;

said security server system transferring said buyer information to a first one of said merchant server system, a payment server system and a delivery server system, wherein said first system removes the document associated with the first system and transmits the remaining documents to a second one of said merchant server system, said payment server system and said delivery server system, wherein said second system removes the document associated with the second system and transmits the remaining document to a third one of said merchant server system, said payment server system and said delivery server system;

wherein said security server system encrypts said buyer information using an encryption key in which only said payment server system is capable of decrypting said payment document and only said delivery server system is capable of decrypting said address document.

27. (original) A method for performing secure transactions over a communication network comprising:

A. establishing a connection between a buyer system and a merchant server system over said communications network to initiate a purchase transaction;

B. said buyer system selecting an item offered for sale by said merchant server system;

C. said buyer system transmitting buyer information to a security server system;

D. said security server system encrypting said buyer information using an encryption key that prevents said merchant server system from decrypting said encrypted buyer information;

E. said security server system transmitting said encrypted buyer information to said merchant server system;

F. said merchant server system transmitting at least a portion of said encrypted buyer information to a third server system for processing during said purchase transaction; and

G. said third server system decrypting said at least a portion of said encrypted buyer information before processing said information.

28. (amended) A method for identifying a party comprising:

A. obtaining a plurality of identifying indicia from each of a plurality of parties;
B. performing a one-way hash function on each of said plurality of identifying indicia to form a plurality of hashed identifiers, wherein a particular output of said one-way hash function is unique to a particular input of said hash function;

C. forming an array of hashed identifiers for each of said plurality of parties, wherein each array includes a number of hashed identifiers that are unique to each party;

D. receiving an identifying indicium from a party;

E. performing said hash function on said indicium to form a hashed indicium;

F. parsing each of said arrays to determine if said hashed indicium coincides with a hashed identifier therein;

G. determining which, if any, of said arrays contains a match ~~coincidence~~ between said hashed indicium and a hashed identifier;

wherein, upon one match occurring ~~if only one coincidence occurs~~, the method comprises:

——— H. identifies ~~identifying~~ a unique party from said plurality of parties based said ~~coincidence~~ match between said hashed indicium and said hashed identifier; and

wherein, upon two or more matches occurring ~~if more than one coincidence occurs~~, the method comprises:

——— I. repeats ~~repeating~~ steps D-G until one of said arrays contains a set of matches ~~coincidences~~ that none of the other arrays contain; and

H[J]. identifying a unique party from said plurality of parties based on said set of matches ~~coincidences~~.

29. (amended) A method for identifying a party comprising:

in a security server system including a computer processor and associated memory, said security server system being selectively couplable to a second server system, including a computer processor and associated memory, over a communications network, performing the steps of:

A. obtaining a plurality of identifying indicia from each of a plurality of parties;

B. performing a one-way hash function on each of said plurality of identifying indicia to form a plurality of hashed identifiers, wherein a particular output of said one-way hash function is unique to a particular input of said hash function;

C. forming an array of hashed identifiers for each of said plurality of parties, wherein each array includes a number of hashed identifiers that are unique to each party; and

in said second server system, performing the steps of:

D. receiving an identifying indicium from a party;

E. performing said hash function on said indicium to form a hashed indicium;

F. parsing each of said arrays to determine if said hashed indicium matches ~~coincides~~ with a hashed identifier therein;

G. determining which, if any, of said arrays contains a match ~~coincidence~~ between said hashed indicium and a hashed identifier;

wherein, upon one match occurring ~~if only one coincidence occurs~~, the method ~~comprises:~~

~~—H. identifies identifying~~ a unique party from said plurality of parties based said match ~~coincidence~~ between said hashed indicium and said hashed identifier; ~~and~~

wherein, upon two or more matches occurring ~~if more than one coincidence occurs~~, the method ~~comprises:~~

~~—I. repeats repeating~~ steps D-G until one of said arrays contains a set of matches ~~coincidences~~ that none of the other arrays contain; and

J. identifying a unique party from said plurality of parties based on said set of matches

Applicant: J. McIsaac
Serial No.: 09/826,052
Filed: 3 April 2001

Atty Docket: 057673- 0015 (QUAL-110)

~~coincidences.~~